

# Disclosure de Informações sobre Segurança do Internet Banking em sites Bancários: o Papel da Internet na Difusão de Inovações

Received: 14/09/2019

Approved: 18/12/2019

**1Fernanda Francielle de Oliveira Malaquias**

**2Daniela De Santi Silva**

## Resumo

**Objetivo do estudo:** Esse artigo teve como objetivo analisar o nível de *disclosure* de informações sobre segurança do Internet Banking em sites bancários, bem como os seus determinantes.

**Metodologia:** A avaliação do nível de *disclosure* baseou-se em um framework com 25 itens, que se dividem em medidas físicas, administrativas e técnicas. Foram adotadas as abordagens quantitativas (estatística descritiva e análise de regressão multivariada) e qualitativa (análise de conteúdo) para análise dos dados.

**Originalidade/Relevância:** Considerando que a segurança é um dos principais determinantes da adoção do Internet Banking, esse estudo visa ampliar a discussão sobre tecnologias bancárias e segurança da informação, focando em um tópico que ainda tem sido pouco explorado no cenário brasileiro.

**Principais resultados:** Os principais resultados evidenciaram que o nível de informações sobre segurança divulgadas pelos bancos em seus sites é baixo. Bancos com maior número de agências, com maior rentabilidade e bancos privados apresentaram melhores níveis de *disclosure*.

**Contribuições teóricas/metodológicas:** No campo teórico, o estudo traz contribuições para a literatura ao abordar um tema ainda pouco explorado, especialmente no Brasil. Ademais, esta pesquisa aborda este tema considerando uma perspectiva tanto quantitativa quanto qualitativa, o que permite maior detalhamento sobre os itens a serem considerados pelas instituições financeiras ao oferecerem serviços eletrônicos aos seus clientes.

**Contribuições para a gestão:** Os resultados da pesquisa podem contribuir para que os bancos avaliem e melhorem o nível de informações que estão sendo divulgadas para seus clientes a fim de aumentar a confiança dos consumidores no Internet Banking e, consequentemente, a difusão dessa tecnologia.

**Palavras-chave:** *Disclosure* Baseado na Web. Segurança das Informações. Tecnologias Bancárias.

## Como Citar:

Malaquias, F., & Silva, D. (2020). Disclosure de Informações sobre Segurança do Internet Banking em sites Bancários: o Papel da Internet na Difusão de Inovações. Future Studies Research Journal: Trends and Strategies [FSRJ], 12(1), 112-129. doi: <https://doi.org/10.24023/FutureJournal/2175-5825/2020.v12i1.456>

<sup>1</sup> Universidade Federal de Uberlândia – UFU, Minas Gerais, (Brasil). E-mail: [fernandafrancielle@gmail.com](mailto:fernandafrancielle@gmail.com)  
Orcid id: <https://orcid.org/0000-0001-7997-530X>

<sup>2</sup> Universidade Federal de Uberlândia – UFU, Minas Gerais, (Brasil). E-mail: [daniela.santisilva@gmail.com](mailto:daniela.santisilva@gmail.com)

# D

## isclosure of Information about Internet Banking Security on Bank Websites: The Role of the Internet in the Diffusion of Innovations

### Abstract

**Purpose:** This paper aims to analyze the level of disclosure of information about Internet Banking security on bank websites, as well as its determinants.

**Methodology:** The analysis of the disclosure level was based on a framework consisting of 25 items divided into physical, administrative and technical measures. We adopted quantitative (descriptive statistics and multivariate regression analysis) and qualitative (content analysis) approaches for data analysis.

**Originality / Value:** Considering that security is one of the main determinants of Internet Banking adoption, this study aims to expand the discussion on banking services and information security, focusing on a topic that has still been little explored in the Brazilian scenario.

**Findings:** The main results showed that the level of security information disclosed by banks on their websites is low. Banks with a greater number of branches, with higher profitability and private banks showed better levels of disclosure.

**Theoretical / methodological contributions:** At the theoretical level, the study brings contributions to the literature by addressing a topic that has been little explored, especially in Brazil. In addition, this research addresses this issue considering both a quantitative and qualitative perspective, which allows a greater detail on the items to be considered by financial institutions when offering electronic services to their customers.

**Managerial implications:** The results of the study may help banks to assess and improve the level of information being disclosed to their customers in order to increase consumer trust in Internet Banking and, consequently, the diffusion of this technology.

**Keywords:** Web-based Disclosure; Information Security; Banking Technologies.

### How to cite the article:

Malaquias, F., & Silva, D. (2020). Disclosure of Information about Internet Banking Security on Bank Websites: The Role of the Internet in the Diffusion of Innovations. *Future Studies Research Journal: Trends and Strategies*, 12(1), 112-129. doi:<https://doi.org/10.24023/FutureJournal/2175-5825/2020.v12i1.456>

## 1. Introdução

O surgimento da Internet provocou uma revolução no setor financeiro, alterando significativamente a maneira como os serviços bancários são acessados (Hanafizadeh, Keating & Khedmatgozar, 2014). Atualmente, por meio do canal conhecido como Internet Banking, as pessoas podem executar transações bancárias tais como pagamentos, transferências e verificação de saldos e extratos, de uma forma eficiente a qualquer hora do dia, independentemente da sua localização física (Hanafizadeh et al., 2014).

Entretanto, apesar da conveniência e comodidade proporcionadas pelo Internet Banking, muitas pessoas têm receio de utilizar esse canal para realizar suas transações bancárias e a sua adoção está abaixo das expectativas (Dumicic; Casni & Palic, 2015; Aboobucker & Bao, 2018). Para que os usuários adotem o Internet Banking, é necessário haver confiança, mas o fato de envolver dados pessoais e de não haver um contato físico faz com que muitos usuários evitem a sua adoção (Lim, Yeow & Yuen, 2010; Aboobucker & Bao, 2018).

De acordo com a Teoria da Difusão de Inovações, a disseminação de informações nos meios de comunicação em massa é essencial para a difusão de inovações (Rogers, 1995). Atualmente, um dos meios de comunicação que se destaca é a Internet que tem sido utilizada pelas empresas com propósitos diversos, dentre eles a interação com os clientes e a divulgação de produtos e informações nos sites corporativos. (Gajewski & Li, 2015; Giau et. al, 2016).

No caso do Internet Banking, Munõz-Leiva et al. (2010), apontam que a divulgação de informações sobre a conformidade do banco com as leis e comentários de outros clientes disponíveis no site do banco podem aumentar a confiança dos clientes, especialmente quando acompanhadas de informações sobre medidas de segurança e garantias de devolução.

Lim et al. (2010), também ressaltam que a fim de mostrar que possuem um canal de Internet Banking seguro, os bancos devem se preocupar com as informações sobre segurança que eles divulgam nos seus sites. Os autores desenvolveram um framework com 25 itens relacionados à segurança do Internet Banking que deveriam ser evidenciados pelos bancos. Esses itens foram divididos em três categorias: (a) Medidas Físicas: medidas para limitar o acesso físico aos dados dos clientes; (b) Medidas Administrativas: medidas adotadas para proteger as informações dos clientes; e (c) Medidas Técnicas: medidas de caráter técnico que ajudam a proteger as informações. Foram analisados bancos da Austrália e da Malásia e concluiu-se que

há diferenças nos níveis de evidenciação entre os bancos dos dois países que podem ser explicadas por fatores culturais.

Nesse contexto, considerando-se a importância da divulgação de informações sobre segurança do Internet Banking e considerando-se que bancos de diferentes países apresentam níveis diferentes de evidenciação, o presente artigo tem como objetivo identificar o nível de *disclosure* de informações sobre segurança do Internet Banking nos sites dos bancos brasileiros que oferecem esse serviço. Para a mensuração do nível de *disclosure*, foi utilizado o framework proposto por Lim et al. (2010). A referida mensuração também levou em consideração as três sub-categorias do framework (medidas físicas, administrativas e técnicas). Como objetivo secundário, analisou-se a relação entre o nível de *disclosure* e as características dos bancos, dentre elas, o tamanho (medido pela quantidade de agências), a performance (medida pela rentabilidade), e o tipo de controle acionário (se público ou privado, se nacional ou estrangeiro).

Os resultados da pesquisa podem contribuir para que os bancos avaliem e melhorem o nível de informações que estão sendo divulgadas para seus clientes a fim de aumentar a confiança dos consumidores no Internet Banking e consequentemente a difusão dessa tecnologia. O estudo também traz contribuições para a literatura ao abordar um tema ainda pouco explorado, especialmente no Brasil.

## 2. Revisão da Literatura

Devido à importância da segurança em Sistemas de Informação, a análise dos fatores associados à segurança e à confiança dos usuários do Internet Banking tem sido o objeto de vários estudos. De acordo com uma pesquisa realizada no Reino Unido, a segurança é o fator mais importante que afeta a taxa de adoção de Internet Banking (Shanmugam, Wang, Bugshan & Hajli, 2015). Essa preocupação com a segurança se justifica na medida em que um sistema perfeitamente seguro não existe e os bancos, assim, como outras organizações, são vulneráveis a cyber-ataques (Lim et al., 2010).

De fato, um sistema, se não for programado corretamente pode apresentar vulnerabilidades nos mecanismos de segurança permitindo que os indivíduos não autorizados acessem informações privadas para ganho pessoal ou para fins maliciosos (French, 2012). Dessa forma, bancos com instalações e sistemas com menor nível de segurança costuma ser mais suscetíveis a cyber-ataques (Lim et al., 2010).

Conforme apontado por French (2012), embora a segurança do Internet Banking continue aumentando em sofisticação para proteger os usuários contra ameaças, há ainda comportamentos de segurança pobres por parte dos usuários. Nesse sentido, a

pesquisa de Negas, Lopes e Negas (2013) objetivou identificar o perfil dos usuários do Internet Banking e avaliar as percepções de riscos e segurança relativas a este serviço. Os autores concluíram que fatores tais como a idade, a inexperiência na utilização da plataforma da Internet e a desvalorização ou desconhecimento da real importância da segurança das informações levam a atitudes incorretas perante o risco.

Ao analisar questões relacionadas à confiança e desconfiança na Web, Seckler, Forde, Tuch & Opwis (2015) concluíram que o conteúdo de um site pode afetar a confiança e a desconfiança dos usuários: questões relacionadas à privacidade e design tem um efeito sobre a desconfiança, enquanto sinais de segurança aumentam a confiança. Além disso, o estudo mostrou que a confiança de um usuário tem base em fatores sociais tais como recomendações e comentários de amigos. Com relação ao Internet Banking Abraham e Bao (2018) observaram que a usabilidade do site e a percepção de confiança são aspectos que podem se constituir em fatores obstrutivos do uso do Internet Banking.

A pesquisa de Hernandez e Mazzon (2007), realizada no Brasil, identificou que itens relativos à segurança e privacidade, dentre eles as preocupações relacionadas com o risco de roubo de informações, roubo de identidade ou venda de informações privadas influenciam significativamente a adoção do Internet Banking. O estudo de Ong e Lin (2015) concluiu que a segurança percebida é um importante antecedente da confiança e do risco percebido, tendo efeitos diretos e indiretos sobre a adoção do Internet Banking. Por isso, sugerem que a gestão do Internet Banking deve colocar mais ênfase na implementação de novos mecanismos de segurança da informação e métodos de marketing para aumentar a percepção da segurança dos indivíduos.

Já o estudo de Twun e Ahenkora (2012) identificou que os usuários veem o Internet Banking como mais seguro do que os não usuários. A percepção de segurança do Internet Banking foi influenciada positivamente pela confiança no sistema de Internet Banking, pela confiança no fornecedor e pela disponibilidade de informação e educação.

Disponibilização de informações e educação também foram apontadas por Redlinghuis e Rensleigh (2010), como o foco principal dos investimentos a serem realizados pelas instituições financeiras. De acordo com os autores, as informações sobre o Internet Banking devem ser de fácil acesso e devem ser divulgadas de uma maneira que faça sentido para os diversos tipos de clientes, especialmente em países com grande diversidade cultural.

A falta de informações já foi apontada como uma das razões para a não adoção do Internet Banking (Munõz-Leiva et al., 2010; Cruz, Filgueiras Neto, Munoz-Gallego

& Laukkanen, 2010). Por isso, a evidenciação de informações sobre o Internet Banking é um tema relevante, se tornando o alvo da presente pesquisa. Este tema mostra-se ainda mais oportuno quando se observa a teoria da difusão da inovação, proposta por Rogers (1995), segundo a qual os meios de comunicação em massa (por exemplo, a internet) são fontes de informação relevantes para a difusão de novas tecnologias.

### 3. Modelo de Pesquisa e Hipóteses

O termo *Disclosure* Voluntário se refere à divulgação discricionária de informações financeiras e não financeiras pelas empresas de modo a garantir a transparência corporativa (Scaltrito, 2016). Devido ao uso cada vez maior da Internet como meio de divulgação de informações, diversos pesquisadores têm analisado questões relacionadas ao *disclosure* voluntário baseado na web (Debreceeny, Gray & Rahman, 2002; Henchiri, 2011; Bagnoli, Wang & Watts, 2014; Hamrouni, Benkraiem & Karmani, 2017). Em geral, esses estudos mostram que características das empresas como o tamanho, performance, multinacionalidade etc. podem influenciar no nível de *disclosure* voluntário das empresas.

No que se refere ao tamanho das empresas, os estudos anteriores identificaram que empresas maiores apresentam maiores níveis de *disclosure*. Isso ocorre porque empresas maiores tem maior visibilidade no mercado, o que as estimula a divulgar informações para melhorar sua imagem e reputação (Debreceeny et al., 2002). Além disso, empresas maiores podem ter melhores sistemas e mais recursos para divulgar informações via web (Lopes & Rodrigues, 2007; Henchiri, 2011). Com base na literatura, Gajewski e Li (2015) apontam que o tamanho das empresas tem sido considerado o principal determinante da evidenciação de informações pela web. No presente trabalho, o tamanho dos bancos será medido pela quantidade de agências. Considerando os estudos anteriores tem-se, então, a seguinte hipótese:

**H<sub>1</sub>:** Bancos com maior número de agências apresentam maior nível de *disclosure* sobre segurança do Internet Banking.

Além do tamanho, a performance das empresas também pode influenciar no nível de *disclosure*. O estudo de Bagnoli et al. (2014), identificou que empresas com dificuldade financeira evidenciam menos informações financeiras em seus sites corporativos. Boubaker, Lakhal e Nekhili (2011) também identificaram que as empresas mais rentáveis divulgam mais informações em seus sites.

De acordo com Henchiri (2011), a fim de atrair ou reter investidores as empresas tendem a divulgar mais informações quando as informações são favoráveis. Segundo Oliveira, Rodrigues e Craig (2006), os modelos teóricos têm estabelecido uma relação

positiva entre o *disclosure* e a performance das empresas. Assim, tem-se a seguinte hipótese:

**H<sub>2</sub>:** Bancos com melhor performance apresentam maior nível de *disclosure* sobre segurança do Internet Banking.

Sobre o tipo de controle (público ou privado), algumas pesquisas têm mostrado que empresas privadas evidenciam mais informações do que as públicas. O estudo de Nie, Liu e Cheng (2016) realizado na China, por exemplo, identificou que empresas com maior controle governamental tem menores níveis de *disclosure*. O estudo de Abraham, Marston e Jones (2015) também mostrou uma relação negativa entre controle governamental e *disclosure* corporativo na Índia. De acordo com os autores, empresas com controle governamental em todo o mundo nem sempre se pautam pela eficiência e pelo critério econômico. Pressupõe-se, com base nos dois estudos mencionados, que os sites dos bancos privados podem conter maior nível de detalhamento sobre segurança do Internet Banking. Dessa forma, tem-se a seguinte hipótese:

**H<sub>3</sub>:** Bancos privados apresentam maior nível de *disclosure* sobre segurança do Internet Banking do que os bancos públicos.

De acordo com Lopes e Rodrigues (2007), empresas com operações internacionais precisam mostrar aos seus *stakeholders* (clientes, fornecedores e governo) que são boas empresas, apresentando bons níveis de *disclosure*. Essas empresas “são mais propensas a aumentar o seu *disclosure* voluntário para mostrar sua presença internacional para os *stakeholders*” (Oliveira et al., 2006, p. 17). Desta forma, espera-se que bancos privados com controle estrangeiro tenham maior incentivo para apresentar sites com informações mais completas sobre segurança do Internet Banking a fim de mostrar aos clientes de que se trata de um banco seguro. Considera-se, portanto, que:

**H<sub>4</sub>:** Bancos com controle estrangeiro apresentam maior nível de *disclosure* sobre segurança do Internet Banking em relação aos demais.

#### 4. Metodologia

Para realização dessa pesquisa, de caráter descritivo, foram adotadas as abordagens qualitativa e quantitativa. Conforme será descrito nos parágrafos a seguir, a etapa quantitativa baseou-se na análise da estatística descritiva, análise de quartis



e análise de regressão multivariada, o que permitiu o teste das hipóteses do estudo. No que se refere à análise qualitativa, foi empregada a técnica de Análise de Conteúdo, conforme descrito ao final desta seção.

Em relação à seleção da amostra de bancos, foi acessada a lista de bancos disponível no site do Banco Central contendo informações sobre Bancos comerciais, múltiplos com carteira comercial ou caixa econômica. De posse dessa lista, foram excluídos os bancos que não possuíam Internet Banking (ou cuja página de Internet Banking não tenha sido encontrada), resultando em 72 bancos analisados. Foi realizada uma busca no site de cada banco a fim de encontrar informações relacionadas à segurança do Internet Banking. Todas as informações sobre segurança foram anotadas em um arquivo para posterior análise.

Para a mensuração do nível de *disclosure* sobre segurança do Internet Banking, foi utilizada uma escala denominada *Disclosure* sobre Segurança, composta por 25 questões do framework proposto por Lim et al. (2010), conforme consta no Apêndice A. Não houve tratamento para itens não aplicáveis (Khanna, Palepu & Srinivasan, 2004), uma vez que se entende que todas estas informações são relevantes para aumentar a segurança dos clientes que pretendem utilizar (e que utilizam) o Internet Banking.

Cada um dos itens que foi divulgado no site dos bancos recebeu nota 1; quando não evidenciado, foi atribuída a nota 0. Como a escala é dividida em três categorias de medidas (medidas físicas, medidas administrativas e medidas técnicas), foi calculado o índice de *disclosure* por categoria de medida, bem como o índice de evidenciação global para todas as 25 questões. O cálculo do referido índice envolve o somatório das notas obtidas em cada item dividido pela quantidade total de itens, multiplicado por 100.

Após calcular o índice de evidenciação por banco, aplicou-se a estatística descritiva, com o objetivo de conhecer o comportamento médio do nível de informações sobre segurança relacionadas ao Internet Banking. A estatística descritiva também foi aplicada às variáveis independentes consideradas no modelo quantitativo. Adicionalmente, o nível de *disclosure* foi também analisado com base em quartis.

Ainda na etapa quantitativa, foi empregada a análise de regressão multivariada (Hair Jr. et al., 2005), que permitiu avaliar possíveis fatores relacionados com maiores ou menores níveis de evidenciação de informações de segurança por parte dos bancos da amostra. A análise de regressão, por meio de mínimos quadrados ordinários, foi realizada tendo como variável dependente o índice de *disclosure* geral; em seguida, a mesma análise foi repetida para cada uma das sub-categorias, o que permitiu avaliar



se os fatores relacionados com o índice geral também estão associados com os três tipos de medida de segurança do Internet Banking. Nos modelos estimados, foi avaliada também a estatística de fator de inflação de variância (VIF – *variance inflation factor*) que pode indicar se o modelo possui algum problema relacionado com multicolinearidade.

Foram consideradas quatro variáveis independentes, em linha com as quatro hipóteses previamente estabelecidas no estudo, sendo a sua forma de mensuração apresentada nos parágrafos a seguir:

- Tamanho: o tamanho dos bancos neste estudo foi representado pelo logaritmo natural do número de agências que o respectivo banco possui. Foi utilizado o logaritmo natural com o objetivo de eliminar possíveis efeitos decorrentes de *extreme outliers*;
- Bancos Públicos: é uma variável *dummy* que recebe valor um para bancos com controle do governo e zero para os demais casos. As informações necessárias para essa classificação foram obtidas junto ao sítio eletrônico do Banco Central.
- Rentabilidade: representa uma medida de performance dos bancos, calculada neste estudo mediante o percentual do lucro líquido apresentado pelo banco em relação ao seu ativo total.
- Controle Estrangeiro: variável *dummy*, que recebe valor um para bancos privados que possuem controle estrangeiro e zero para os demais casos. Para essa classificação, as informações foram obtidas junto ao sítio eletrônico do Banco Central do Brasil.

A análise dos resultados também foi realizada com base em procedimentos qualitativos. Na etapa qualitativa, foram seguidos os pressupostos da técnica de Análise de Conteúdo (Krippendorff, 2012). O conteúdo dos websites dos bancos foi codificado e em seguida os códigos foram agrupados em três categorias que foram predefinidas com base no estudo de Lim et al. (2010): Medidas Físicas, Medidas Administrativas e Medidas Técnicas.

## 5. Análise dos Resultados

### 5.1 Análise Quantitativa

No que se refere às variáveis independentes dicotômicas (variáveis *dummies*), a Tabela 1 apresenta as informações relacionadas com suas frequências. Os resultados da referida tabela indicam que a maioria dos bancos componentes da amostra são privados e que 26 dos 72 bancos possuem controle estrangeiro.

**Tabela 1:** Estatística Descritiva das Variáveis Dicotômicas (Binárias)

Tipo	Sim	Não	Total
Banco Público	08	64	72
Contr. Estrangeiro	26	46	72

Notas: As informações para composição desta tabela foram coletadas junto ao sítio eletrônico do Banco Central do Brasil.

A Tabela 2 indica a estatística descritiva para as variáveis independentes escalares, sendo elas Tamanho (representado pelo logaritmo natural do Número de Agências de cada Banco) e Rentabilidade (porcentual do Lucro Líquido em relação ao Ativo Total do Banco). A Tabela 2 também mostra a estatística descritiva tanto para as categorias de medidas (medidas físicas, medidas administrativas e medidas técnicas) quanto para o índice geral com todas as questões.

**Tabela 2:** Estatística Descritiva das Variáveis Escalares

Variáveis	Nº Itens	Nº Bancos	Média	Desvio-Padrão	Mínimo	Máximo
Todos-Itens	25	72	21,222	12,749	0,000	64,000
Medidas-Físicas	3	72	15,278	18,502	0,000	66,667
Medidas-Administrativas	8	72	25,868	12,111	0,000	75,000
Medidas-Técnicas	14	72	19,841	18,071	0,000	64,286
Ln(NumAgencias)	-	72	2,360	2,208	0,693	8,603
Rentabilidade	-	72	-0,205	2,580	-18,862	3,299

Notas: Ln(NumAgencias): representa o logaritmo natural do Número de Agências de cada Banco; Rentabilidade: representa o porcentual do Lucro Líquido em relação ao Ativo Total do Banco.

Conforme pode-se observar na Tabela 2, em média, de acordo com as análises realizadas e critérios estabelecidos para a coleta dos dados, o nível de informações sobre segurança com o internet banking ainda pode ser significativamente melhorado nos sites dos bancos, pois sua média (geral) é de 21,2%. A categoria de análise que parece receber maior atenção por parte dos bancos corresponde a medidas administrativas, com um índice médio de 25,9%. A categoria de medidas administrativas foi também a que registrou o banco com o maior nível de evidenciação (valor máximo = 75%). O menor nível médio de evidenciação foi registrado pela categoria de medidas físicas (média de 15,3%). É importante também observar que em todas as categorias houve bancos que não divulgaram nenhum dos itens avaliados, uma vez que o valor mínimo em todos os quatro casos analisados foi igual a 0%.

Adicionalmente, foi elaborada a Tabela 3, que contém a análise dos índices obtidos considerando medidas de posição que não dependem da média e do desvio-padrão, como é o caso da análise por quartis.

Em linha com a análise quantitativa desenvolvida na Tabela 2, a Tabela 3 também indica um baixo nível de evidenciação sobre segurança do Internet banking por parte

dos bancos. Conforme apontam os resultados, 75% dos bancos (com base no 3º quartil) possuem evidenciação que não alcança a metade dos itens do instrumento de coleta de dados (com base nos critérios adotados para a condução da análise quantitativa por meio do índice de *disclosure*), uma vez que o maior valor para o 3º quartil foi de 33,3%. Outra informação importante é que metade das empresas divulgam, no máximo, 25% dos itens do instrumento de coleta de dados (ou menos que isso), conforme indica a Tabela 3 (especificamente na coluna do 2º Quartil).

**Tabela 3:** Análise do Nível de *Disclosure* por Quartis

Variáveis	Nº Itens	Nº Bancos	1º Quart. (25%)	2º Quart. (50%)	3º Quart. (75%)
Todos-Itens	25	72	12,000	20,000	28,000
Medidas-Físicas	3	72	0,000	0,000	33,333
Medidas-Administrativas	8	72	25,000	25,000	25,000
Medidas-Técnicas	14	72	7,143	14,286	28,571

Com o objetivo secundário de identificar possíveis fatores relacionados com o nível de *disclosure* praticado pelos bancos, foi elaborada uma análise de regressão multivariada e os resultados estão disponíveis na Tabela 4. É oportuno comentar que a estatística de fator de inflação de variância (VIF) não indicou possíveis problemas relacionados com a multicolinearidade.

**Tabela 4:** Análise de Regressão para o Índice de Disclosure Geral (25 itens)

Variáveis	Coef.	Erro-Padrão	Est. T	Signif.
Ln(NumAgencias)	2,828	0,763	3,710	0,000 ***
Banco Público	-10,635	5,316	-2,000	0,049 **
Contr. Estrangeiro	-0,333	2,983	-0,110	0,911
Rentabilidade	1,422	0,534	2,660	0,010 **
Constante	16,143	2,476	6,520	0,000 ***

Núm. Observações: 72

R-quadrado: 23,8%

R-quadrado ajustado: 19,3%

Estatística VIF Média: 1,310

Notas: \*\*\* significante a 1%; \*\* significante a 5%; \* significante a 10%.

Com base nos resultados obtidos pela análise de regressão, pode-se observar que o tamanho dos bancos apresentou relação positiva e significativa a 1% com o nível de *disclosure* sobre elementos de segurança em seus websites. Esse resultado está em consonância com a literatura e sugere que bancos com maior número de agências tendem a divulgar mais informações relacionadas com medidas de segurança do

Internet Banking, o que pode talvez estar relacionado com um possível incentivo para que um maior número de clientes aumente sua confiança nos serviços de internet banking e passem, assim, a adotá-los.

Por sua vez, bancos públicos apresentaram menores níveis médios de *disclosure* considerando um nível de significância estatística de 5%. De acordo com esse resultado, o nível de informações sobre segurança com internet banking é mais detalhado nos sites de bancos privados, o que está em linha com estudos anteriores (Abraham et al., 2015; Nie et al., 2016).

A hipótese sobre um possível incentivo que bancos com controle estrangeiro poderiam ter para ampliar seu nível de evidenciação no cenário brasileiro não foi confirmada. Ou seja, o nível de *disclosure* entre bancos com controle estrangeiro e os demais bancos da amostra mostrou-se como equivalente.

Quanto à rentabilidade, observou-se que bancos com melhores níveis de rentabilidade apresentaram maior nível de evidenciação, o que corrobora os resultados de estudos anteriores (Boubaker et al. 2011; Henchiri, 2011; Bagnoli et al. 2014).

De forma a ampliar o entendimento sobre fatores possivelmente relacionados com o nível de *disclosure* de medidas de segurança, foi elaborada a Tabela 5, que avalia a relação dos fatores utilizados na Tabela 4 com as sub-categorias do índice geral de *disclosure*. Cada coluna resume os resultados com base nos coeficientes e níveis de significância, de acordo com o respectivo nível de medida.

Pelos resultados dispostos na Tabela 5, tem-se que os três tipos de medidas sofrem efeitos diferentes em relação aos possíveis fatores determinantes do nível de evidenciação geral de informações sobre segurança do Internet Banking. Por exemplo, o nível de *disclosure* das medidas físicas não se mostrou associado com nenhum dos quatro fatores; neste ponto, é importante ressaltar que essa sub-categoria foi a que apresentou menor nível de divulgação (conforme Tabela 2), o que indica que o seu nível de informações é equivalente entre bancos maiores e menores, bancos públicos e privados, bancos com controle estrangeiro e controle nacional, e bancos com maior ou menor rentabilidade.

**Tabela 5:** Análise de Regressão para o Índice de *Disclosure* segregado entre os Três Tipos de Medidas

Variáveis	Med. Físicas		Med. Administrativas		Med. Técnicas	
	Coef.	Signif.	Coef.	Signif.	Coef.	Signif.
Ln(NumAgencias)	0.509	0.683	1.753	0.025 **	3.939	0.001 ***
Banco Público	-2.875	0.740	-7.471	0.165	-14.107	0.073 *
Contr. Estrangeiro	-4.823	0.323	-1.715	0.568	1.419	0.745
Rentabilidade	1.093	0.212	1.277	0.020 **	1.575	0.047 **
Constante	16.363	0.000 ***	23.443	0.000 ***	11.925	0.002 ***
Núm. Observações: 72			72		72	
R-quadrado: 4.8%			15.2%		19.4%	
R-quadrado ajustado: 0.0%			10.1%		14.6%	
Estatística VIF Média: 1.310			1.310		1.310	

Notas: Da mesma forma que os resultados obtidos na Tabela 4, a estatística VIF média dos modelos da Tabela 5 foi de 1,310, indicando que uma possível multicolinearidade entre as variáveis independentes não representa uma preocupação no caso destas análises; \*\*\* significante a 1%; \*\* significante a 5%; \* significante a 10%.

De uma maneira geral, os resultados obtidos por meio da análise quantitativa indicam que há significativo espaço para melhorias no nível de evidenciação sobre segurança do Internet Banking dos bancos brasileiros avaliados neste estudo. As evidências indicam que a maioria dos bancos pode incrementar suas informações públicas sobre o tema, e a categoria que parece demandar maior atenção refere-se às medidas físicas, que apresentou menor média, menor valor na análise da mediana (também correspondente ao 2º quartil) e comportamento equivalente entre os diferentes fatores considerados como possíveis determinantes.

## 5.2 Análise Qualitativa

A partir da análise de conteúdo dos sites bancários identificou-se que as medidas físicas são as menos evidenciadas pelos bancos. Muitos bancos apontam em suas políticas de privacidade que os dados dos usuários só serão acessados por funcionários autorizados e que os funcionários que fizerem uso indevido dos dados estão sujeitos a penalidades. Há alguns bancos que evidenciam a existência de medidas que incluem proteções para computadores, arquivos e edificações. Nos sites dos bancos analisados não foram encontradas informações sobre medidas contra espionagem.

A análise dos itens dessa categoria revela que os bancos devem passar a adotar medidas físicas ou aprimorar as medidas físicas existentes. Para aqueles que já adotam tais medidas, as mesmas poderiam ser mais divulgadas nos sites a fim de aumentar a confiança dos usuários.

Com relação às medidas administrativas, a maioria dos bancos divulga suas políticas de privacidade e o uso de diferentes métodos de autenticação, como senhas, códigos e biometria que podem ser utilizadas nos diferentes canais oferecidos. Alguns bancos também apontam que as informações pessoais dos clientes são coletadas e armazenadas de acordo com padrões rígidos de confidencialidade e segurança e que não são repassadas a terceiros, exceto se expressamente autorizado pelo cliente ou por determinação legal. Poucos bancos informam que os funcionários são treinados e capacitados para manuseio de informações pessoais dos clientes. Auditorias também são apontadas por alguns bancos como parte de suas políticas de segurança. O uso de certificados digitais também é divulgado juntamente com o nome da entidade que emite o certificado. Muitos bancos apontam o constante aprimoramento dos seus sites e da navegabilidade, mas em questão de segurança poucos divulgam que os seus sites passam por testes para detectar possíveis vulnerabilidades.

Por fim, com relação às medidas técnicas, as medidas mais evidenciadas se referem ao uso de certificado digital, autenticação via tokens e SMS, bloqueio de senhas, teclado virtual, criptografia e Secure Socket Layer (SSL). Alguns bancos divulgam que por questão de segurança, as senhas costumam ser bloqueadas quando digitadas incorretamente.

O uso de certificado digital geralmente é divulgado como uma medida que funciona como documento de identidade digital. Já a criptografia e o protocolo SSL foram apontados por vários bancos como medidas de segurança que impedem que as informações que transitam entre o computador ou celular do cliente e o banco possam ser interceptadas por outras pessoas de forma indevida. Sobre o uso de firewalls, sistemas de detecção de invasão e antivírus, muitos bancos apenas informam aos clientes sobre a necessidade de instalar esses sistemas em seus computadores pessoais, mas poucos bancos informam que adotam esses sistemas para filtrar o acesso externo e/ou proteger os aplicativos e os dados dentro do banco. O uso de autenticação via tokens e SMS também é informado aos clientes como medidas adotadas para a realização de determinadas operações.

Por meio da análise do conteúdo dos sites, percebe-se que alguns bancos adotam diversas medidas relacionadas às três categorias analisadas e divulgam essas informações de forma mais completa.

Entretanto, há bancos que não divulgam tais informações, não sendo possível identificar por meio de seus sites se as medidas são adotadas ou não, o que pode afetar a confiabilidade dos clientes nos seus sistemas.

## 6. Considerações Finais

Esse artigo teve como objetivo identificar o nível de *disclosure* sobre segurança do Internet Banking nos sites dos bancos brasileiros que oferecem esse serviço. Por meio de uma análise tanto qualitativa quanto quantitativa identificou-se que, embora alguns bancos divulguem informações mais completas sobre as medidas de segurança adotadas, o panorama geral indica carência sobre essas informações com base nas três categorias consideradas na análise empírica.

A análise dos determinantes também evidenciou que o *disclosure* de informações sobre segurança do Internet Banking mostrou-se relacionado às características dos bancos. Bancos maiores, com controle privado e com melhor performance divulgaram mais informações.

Conforme mencionado anteriormente, a divulgação de informações aos clientes pode contribuir para uma maior adoção do Internet Banking. Portanto é importante que os bancos não apenas adotem medidas de segurança, mas também informem seus clientes sobre as medidas adotadas. Nesse ponto, esse estudo enfatiza o papel da Internet como um meio de baixo custo que pode ser utilizado pelos bancos para esclarecer os clientes sobre a segurança de seus sistemas.

Dentre as três categorias, a que merece mais atenção dos bancos se refere às medidas físicas, já que poucas informações a respeito dessas medidas foram encontradas. Sobre as medidas administrativas e técnicas, alguns bancos informam não apenas sobre o uso das mesmas, mas também sobre o objetivo a que se destinam. Isso é importante para tornar os usuários mais informados e seguros sobre os sistemas. Como alguns bancos provavelmente adotam tais medidas, mas não as divulgam ou não as divulgam de maneira fácil de ser encontrada, sugere-se que tais informações sejam apresentadas nos seus sites com fácil acesso para os clientes.

Essa pesquisa apresenta implicações tanto práticas quanto teóricas. Primeiramente no campo prático, o estudo contribui para que os bancos possam avaliar e aprimorar o nível de informações sobre segurança divulgadas nos seus sites. No campo teórico, esse estudo permite ampliar as pesquisas sobre serviços bancários e segurança da informação, tema que ainda tem sido pouco explorado no cenário brasileiro.

Ademais, esta pesquisa aborda este tema considerando uma perspectiva tanto quantitativa quanto qualitativa, o que permite maior detalhamento sobre os itens a serem considerados pelas instituições financeiras ao oferecerem serviços eletrônicos aos seus clientes. Estes itens, de maneira geral, quando evidenciados com detalhes e



de maneira clara, podem apresentar um efeito positivo na difusão dessa tecnologia (internet banking), que possui benefícios tanto para os clientes quanto para os bancos.

Como limitações do trabalho, ressalta-se que a análise foi realizada com base em informações que foram encontradas durante as pesquisas nos websites. É possível que alguns bancos divulguem informações que não tenham sido encontradas pelos pesquisadores. Como pesquisa futura sugere-se a realização de um estudo com usuários do Internet Banking com o objetivo de identificar as informações que os mesmos consideram relevantes na hora de decidir sobre o uso de sistemas bancários virtuais.

## Referências

Aboobucker, I. & Bao, Y. (2018) What obstruct customer acceptance of internet banking? Security and privacy, risk, trust and website usability and the role of moderators. *Journal of High Technology Management Research*, 29(1), 109–123.

Abraham, S., Marston, C. & Jones, E. (2015) Disclosure by Indian companies following corporate governance reform. *Journal of Applied Accounting Research*, 16(1), 114-137.

Bagnoli, M., Wang, T. & Watts, S. G. (2014) How do corporate websites contribute to the information environment? Evidence from the U.S. and Taiwan. *Journal of Accounting and Public Policy*, 33(6), 596-627.

Boubaker, S., Lakhal, F. & Nekhili, M. (2011) The Determinants of Web-based Corporate Reporting in France, *Managerial Auditing Journal*, 27(2), 126 – 155.

Cruz, P., Filgueiras Neto, L. B., Munoz-Gallego, P. & Laukkanen, T. (2010) Mobile banking rollout in emerging markets: evidence from Brazil. *International Journal of Bank Marketing*, 28(5), 342-371.

Debreceny, R., Gray, G. L. & Rahman, A. (2002) The Determinants of Internet Financial Reporting, *Journal of Accounting and Public Policy*, 21(4-5), 371–394.

Dumicic, K., Casni, P. & Palic, I. (2015) Multivariate analysis of determinants of Internet banking use in European Union countries. *Central European Journal of Operations Research*, 23(3), 563–578.

French, A. M. (2012) A Case Study on E-Banking Security – When Security Becomes Too Sophisticated for the User to Access Their Information. *Journal of Internet Banking and Commerce*, 17(2), 1-14.

Gajewski J.F. & Li, L. (2015) Can Internet-based Disclosure Reduce Information Asymmetry?, *Advances in Accounting, incorporating Advances in International Accounting*, 31, 115–124.

Giau, A. (2016) Sustainability practices and web-based communication: An analysis of the Italian fashion industry. *Journal of Fashion Marketing and Management*, 20(1), 72-88.

Hair Jr., J.F., Anderson, R. E., Tatham, R.L. & Black, W.C. (2005) *Análise multivariada de dados*. (5a. ed.). Porto Alegre: Bookman.

Hanafizadeh, P., Keating, B. W. & Khedmatgozar, H. R. (2014) A systematic review of Internet banking adoption. *Telematics and Informatics*, 31, 492–510.

Hamrouni, A., Benkraiem, R. & Karmani, M. (2017) Voluntary information disclosure and sellside analyst coverage intensity, *Review of Accounting and Finance*, 16(2), 260-280.

Henchiri, J.E. (2011) Voluntary Web-based Disclosures by Moroccan and Tunisian Companies, *EuroMed Journal of Business*, 6(2), 155-173.

Hernandez, J. M. C. & Mazzon, J. A. (2007) Adoption of internet banking: proposition and implementation of an integrated methodology approach. *International Journal of Bank Marketing*, 25(2), 72 – 88.

Khanna, T., Palepu, K. G. & Srinivasan, S. (2004) Disclosure Practices of Foreign Companies Interacting with U.S. Markets. *Journal of Accounting Research*, 42(2), 475-508.

Krippendorff, K. (2012) *Content Analysis: An Introduction to its Methodology*. Thousands Oak: Sage.

Lim, N., Yeow P. P. H., & Yuen Y. Y. (2010) An Online Banking Security Framework and a Cross-Cultural Comparison. *Journal of Global Information Technology Management*, 13(3), 39-62.

Lopes, P.T. & Rodrigues, L.L. (2007) Accounting for Financial Instruments: An Analysis of the Determinants of Disclosure in the Portuguese Stock Exchange, *The Journal of Accounting*, 42(1), 25-56.

Muñoz-Leiva, F., Luque-Martínez, T. & Sánchez-Fernández, J. (2010) How to improve trust toward electronic banking, *Online Information Review*, 34(6), 907 – 934.

Negas, M. F. C, Lopes, J. M. M. & Negas, E. I. S. R. (2013) Os Utilizadores de Homebanking e Riscos de Segurança mais Relevantes Associados. *Anais da Conferência Ibérica de Sistemas e Tecnologias de Informação*, 8, Lisboa, Portugal.

Nie, L., Liu, H. K. & Cheng, W. (2016) Exploring Factors that Influence Voluntary Disclosure by Chinese Foundations. *Voluntas*, 27, 2374–2400.

Oliveira, L., Rodrigues, L.L. & Craig, R. (2006) Firm-specific Determinants of Intangibles Reporting: Evidence from the Portuguese Stock Market, *Journal of Human Resource Costing and Accounting*, 10(1), 11-33.

Ong C.S. & Lin, Y. L. (2015) Security, Risk, and Trust in Individuals' Internet Banking Adoption: an Integrated Model. *International Journal of Electronic Commerce Studies*, 6(2), 343-356.

Redlinghuis, A. & Rensleigh, C. (2010) Customer perceptions on Internet banking information protection. *South Africa Journal of Information Management*, 12(1), 1-6.

Rogers, E. M. *Diffusion of Innovations*. (1995) (4a ed.), New York: Free Press.

Seckler, M., Heinz, S., Forde, S., Tuch, A. N. & Opwis, K. (2015) Trust and distrust on the web: User experiences and website Characteristics. *Computers in Human Behavior*. 45, 39–50.

Scaltrito, D. (2016) Voluntary disclosure in Italy: Firm-specific determinants an empirical analysis of Italian listed companies. *EuroMed Journal of Business*. 11(2), 272-303.

Shanmugam, M., Wang, Y. Y., Bugshan, H. & Hajli, N. (2015) Understanding customer perceptions of internet banking: the case of the UK. *Journal of Enterprise Information Management*, 28(5), 622 – 636.

Twum, F. & Ahenkora, K. (2012) Internet Banking Security Strategy: Securing Customer Trust. *Journal of Management and Strategy*, 3(4), 78-83.

**Apêndice A:** Instrumento de Coleta de Dados para Análise do *Disclosure* sobre Segurança

Itens	Tipo de Medida
1 Medidas contra espionagem no escritório	Física
2 Segurança das Instalações	Física
3 Acesso físico às informações dos clientes restrito à pessoas autorizadas	Física
4 Política de Mesa Limpa	Administrativa
5 Treinamento dos funcionários sobre privacidade e confidencialidade	Administrativa
6 Uso de usuário e senha para prevenir acesso não autorizado	Administrativa
7 Logins adicionais com acesso restrito	Administrativa
8 Indicação do emitente do certificado digital	Administrativa
9 Auditoria interna e externa dos sistemas e da infraestrutura de TI	Administrativa
10 Política e armazenamento de informações	Administrativa
11 Revisões e testes regulares das tecnologias para melhorar a segurança	Administrativa
12 Bloqueio automático após várias tentativas de logins mal sucedidos	Técnica
13 Bloqueio da senha após logout	Técnica
14 Sistemas de detecção de invasão	Técnica
15 Monitoramento de atividades suspeitas	Técnica
16 Time-out de sessão	Técnica
17 Uso de criptografia em geral	Técnica
18 Uso do padrão de criptografia de 128 bits	Técnica
19 Uso de certificado digital	Técnica
20 Uso de Secure Socket Layer (SSL)	Técnica
21 Uso de Firewalls	Técnica
22 Uso de anti-vírus	Técnica
23 Uso de códigos de autenticação via tokens de segurança	Técnica
24 Uso de códigos de autenticação via mensagens SMS	Técnica
25 Uso de teclado virtual	Técnica

Fonte: Lim, Yeow e Yuen (2010).